OVAL

Integration and Automation

Andrew Buttner

September 19, 2006

MITRE

© 2006 The MITRE Corporation. All rights reserved

Agenda

- What is OVAL
- Why OVAL
- The Language
- Use Cases
- NIST
- OVAL Compatibility

© 2006 The MITRE Corporation. All rights reserved

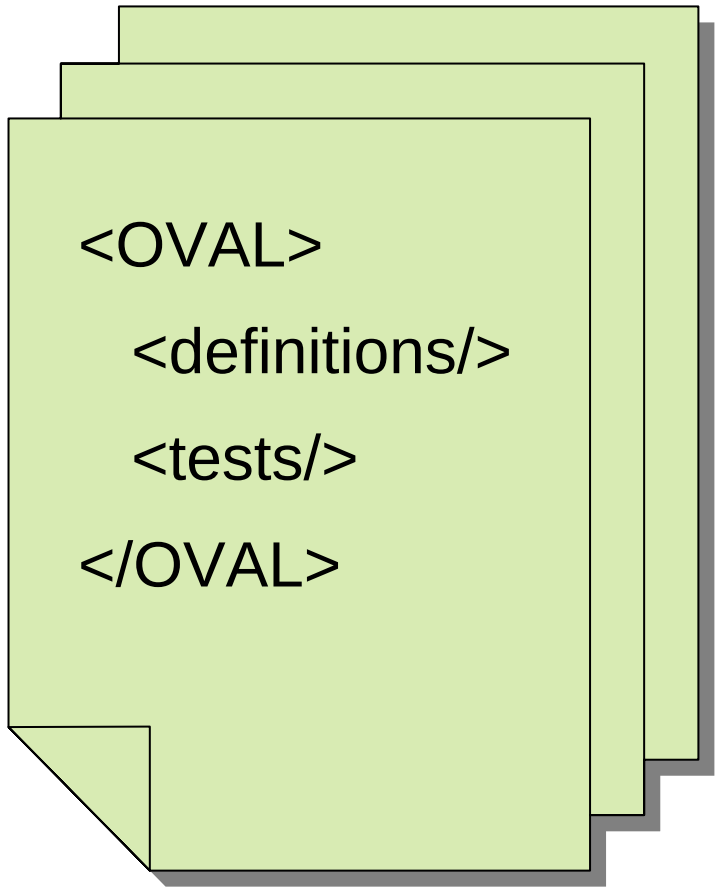
What Is OVAL?

- **OVAL Language**
  - express specific machine states
  - standardize the transfer of information
  - XML based defined by XML Schema
- **OVAL Repository**
  - promote open and publicly available content
  - central meeting place
- **open community standard**
  - to facilitate sharing
  - open up the details
  - utilize community expertise
- **sponsored by the US-CERT at the Department of Homeland Security**

© 2006 The MITRE Corporation. All rights reserved

Why OVAL

- machine readable document
  - less errors due to human translation
- immediate response
  - through automation
- interoperability
  - vendor neutral language
- open to the user

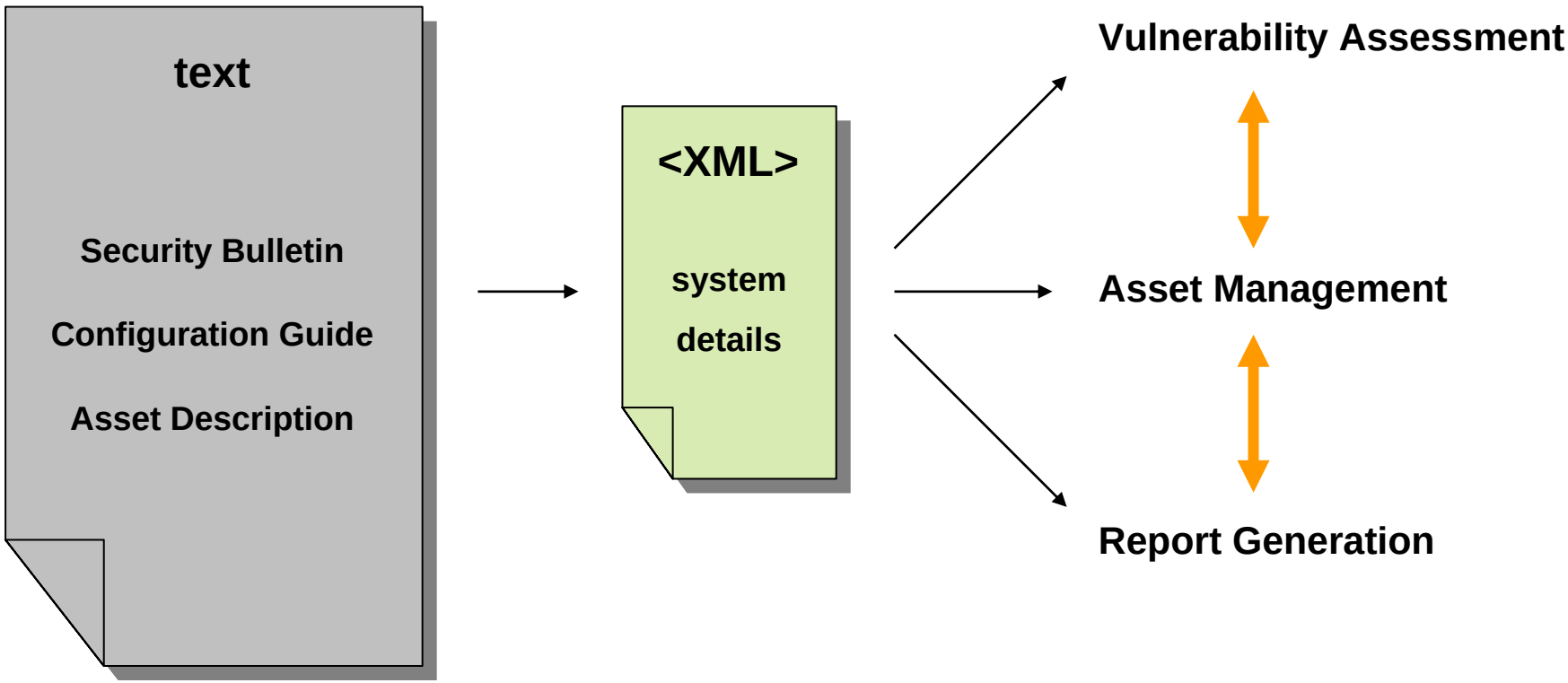


© 2006 The MITRE Corporation. All rights reserved

System Details

© 2006 The MITRE Corporation. All rights reserved

The Language



MITRE

© 2006 The MITRE Corporation. All rights reserved

OVAL Schema

- **Three separate XML schemas**
  - **OVAL System Characteristics Schema**
  - **OVAL Definition Schema**
  - **OVAL Results Schema**

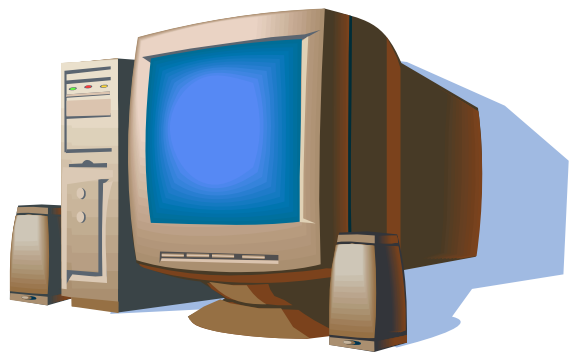
- **Schema structure**
  - **core schema**
  - **individual component schemas**

Natural for software authors to provide expertise in shaping these schemas.

© 2006 The MITRE Corporation. All rights reserved

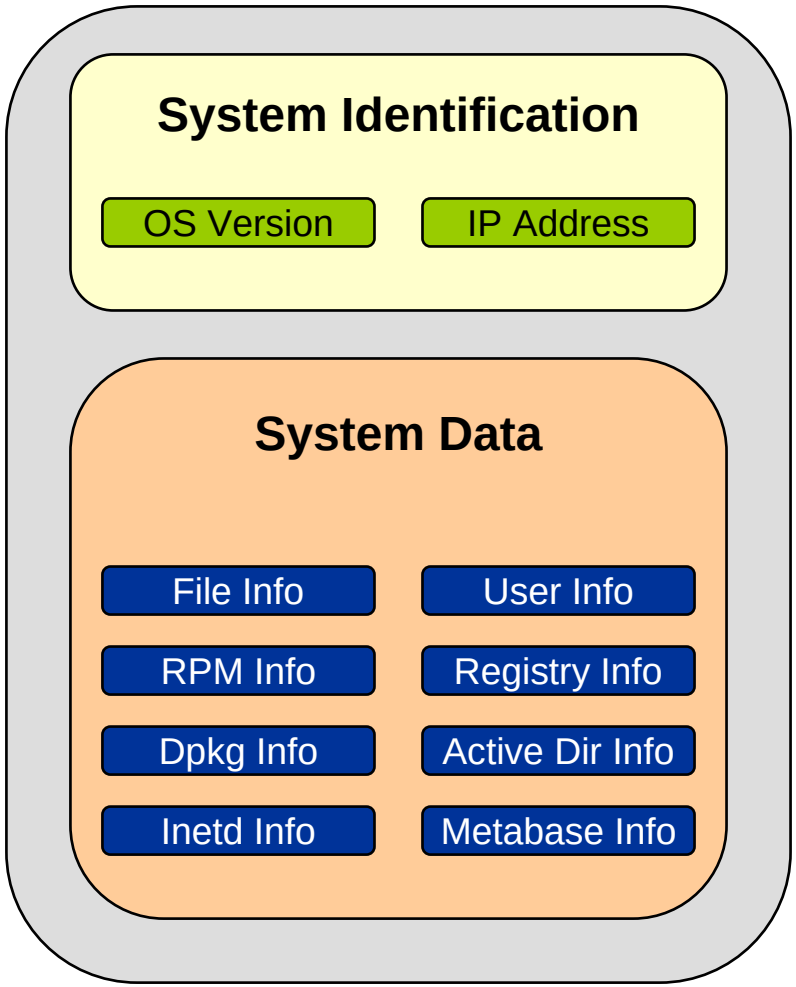
OVAL System Characteristics

- XML encoding of the details of a system
  - file versions
  - running processes
  - patches installed
  - etc.
- provides a snapshot of the system
  - save for auditing purposes
  - use for analysis



© 2006 The MITRE Corporation. All rights reserved

OVAL System Characteristics



MITRE

© 2006 The MITRE Corporation. All rights reserved

OVAL Definition

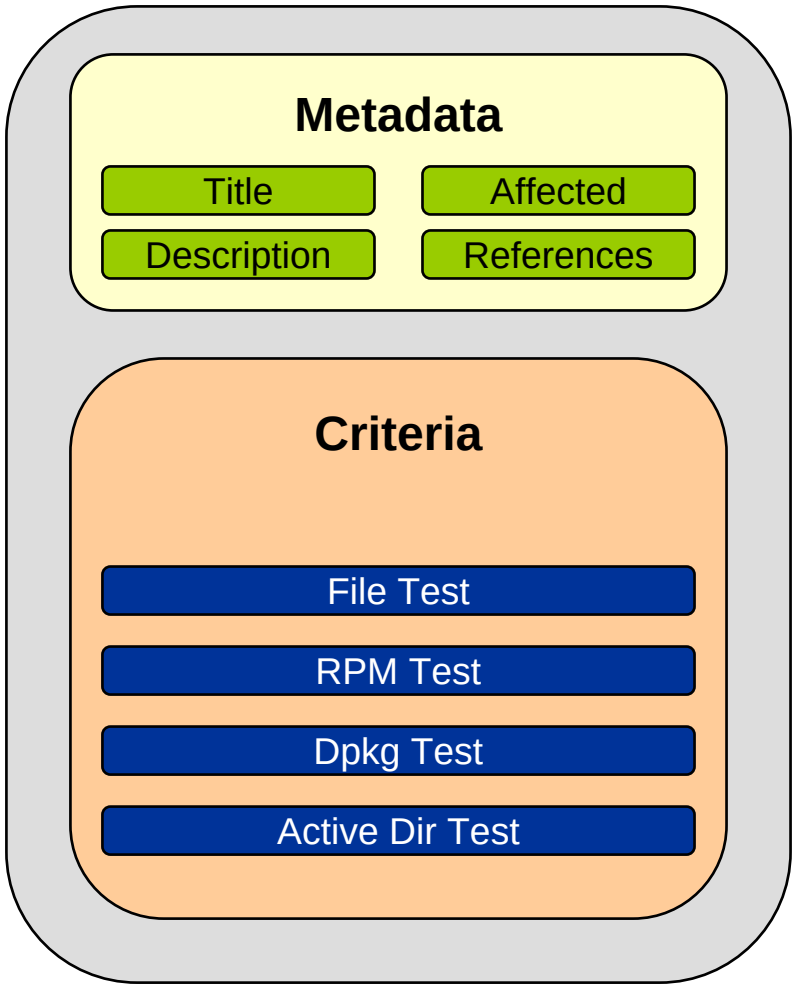
- **the specific details that make up system state you want to test**

- **composed of meta-data …**
  - **Affected family, platforms, and products.**
  - **Description**
  - **CVE identifier or other reference**

- **… and the set of tests (also known as the criteria)**
  - **Tests can be written to describe any retrievable system information.**
    - registry values
    - file permissions
    - metabase contents

© 2006 The MITRE Corporation. All rights reserved

OVAL Definition



© 2006 The MITRE Corporation. All rights reserved

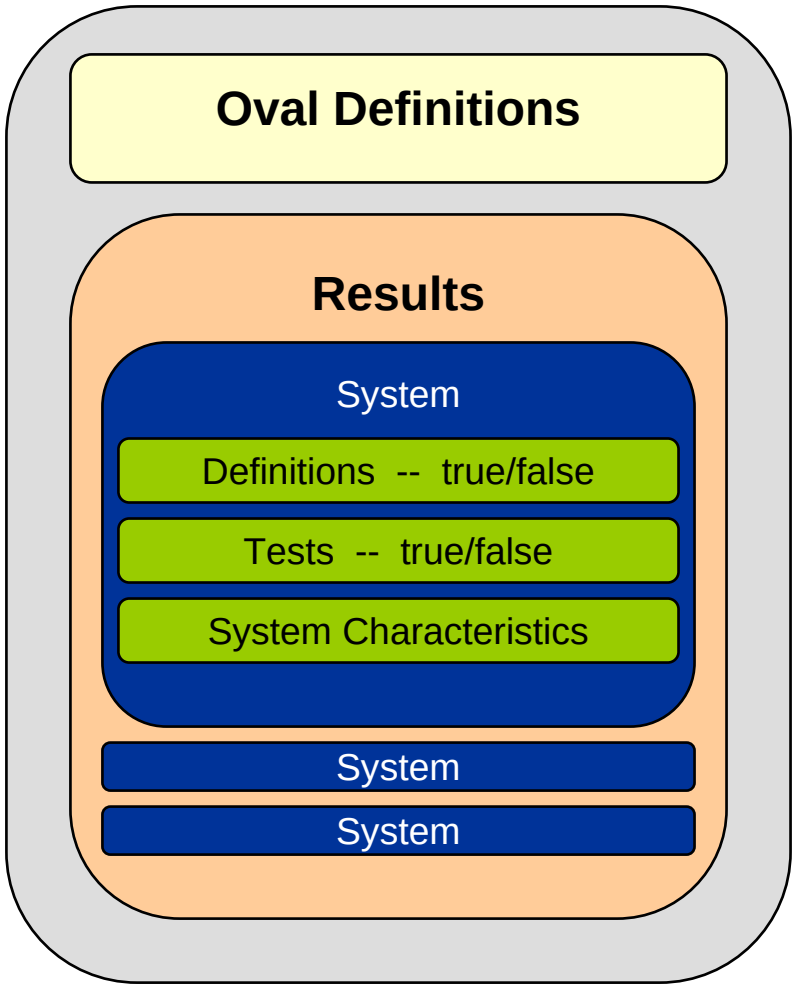
OVAL Results

- XML encoding of the results of an analysis
  - which systems are vulnerable?
  - which systems are non-compliant?
  - which patches should be installed?

- Includes the details
  - why are you vulnerable?
  - why are you non-compliant?
  - why should a patch be installed?

© 2006 The MITRE Corporation. All rights reserved

OVAL Results



MITRE

© 2006 The MITRE Corporation. All rights reserved

The OVAL Process

1

Security advisories

Vendors and leading security organizations publish security advisories that warn of current threats and system vulnerabilities.

Configuration policy

Government agencies such as NSA and NIST develop "Best Practices" policy for system security.

2

OVAL Definitions

Definitions are generated

Specific machine configuration details from Advisory and Policy documents are extracted and encoded as an OVAL Definition.

3

Data collected from computers

OVAL Definitions are structured to indicate what configuration information needs to be collected from an individual system.

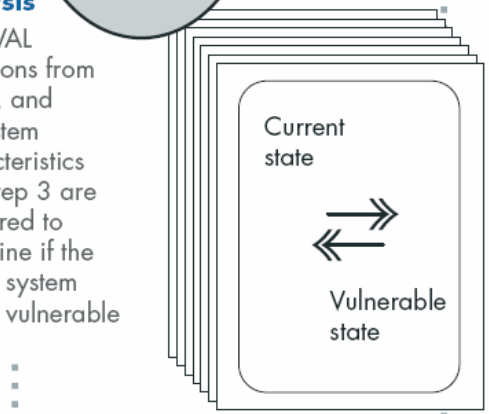
OVAL System Characteristics

4

OVAL Analysis

Analysis

The OVAL Definitions from Step 2, and the System Characteristics from Step 3 are compared to determine if the current system state is vulnerable or not.

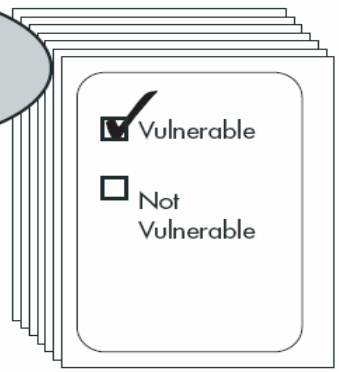


5

Analysis results

Results of analysis are formatted as an OVAL Results document.

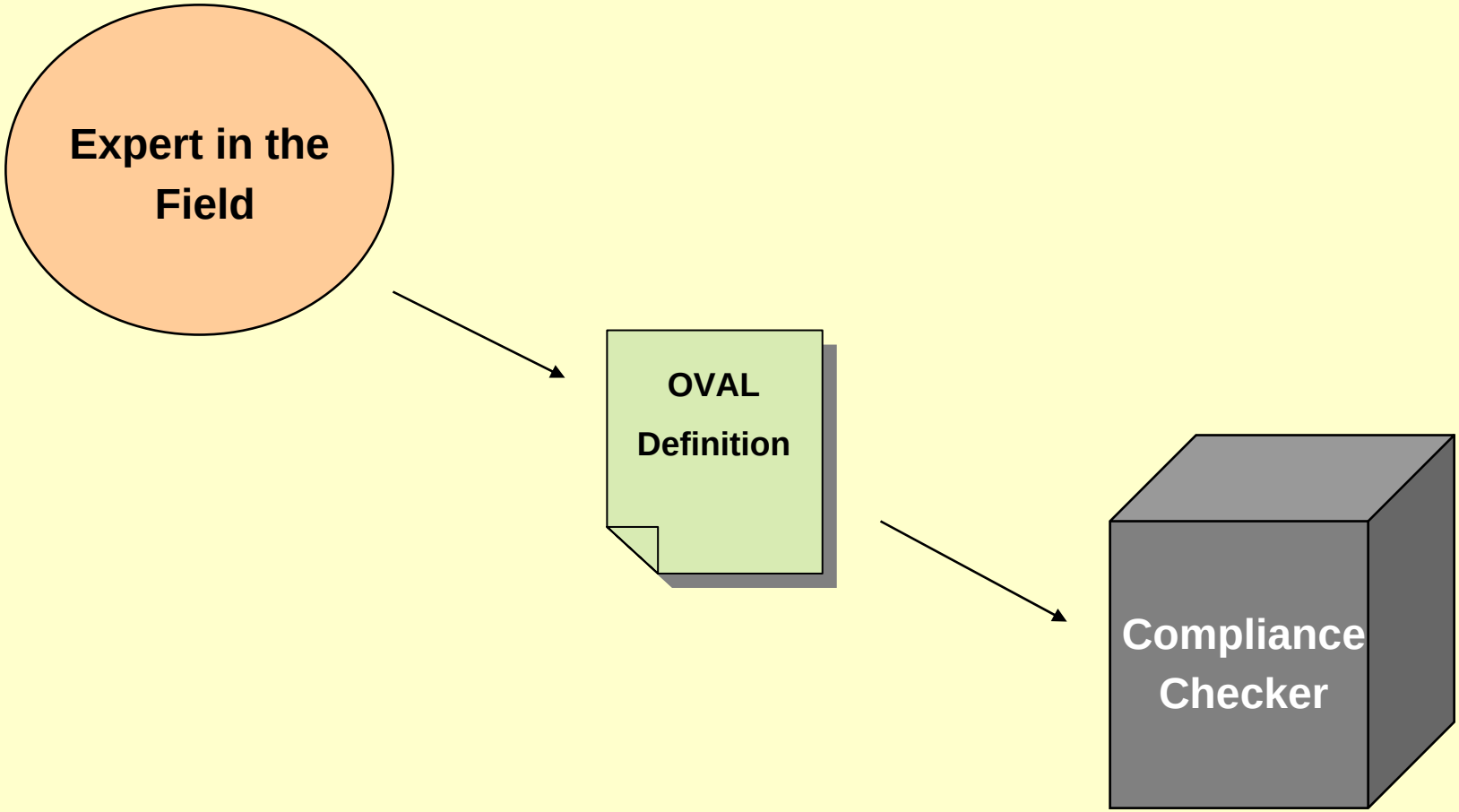
OVAL Results



MITRE

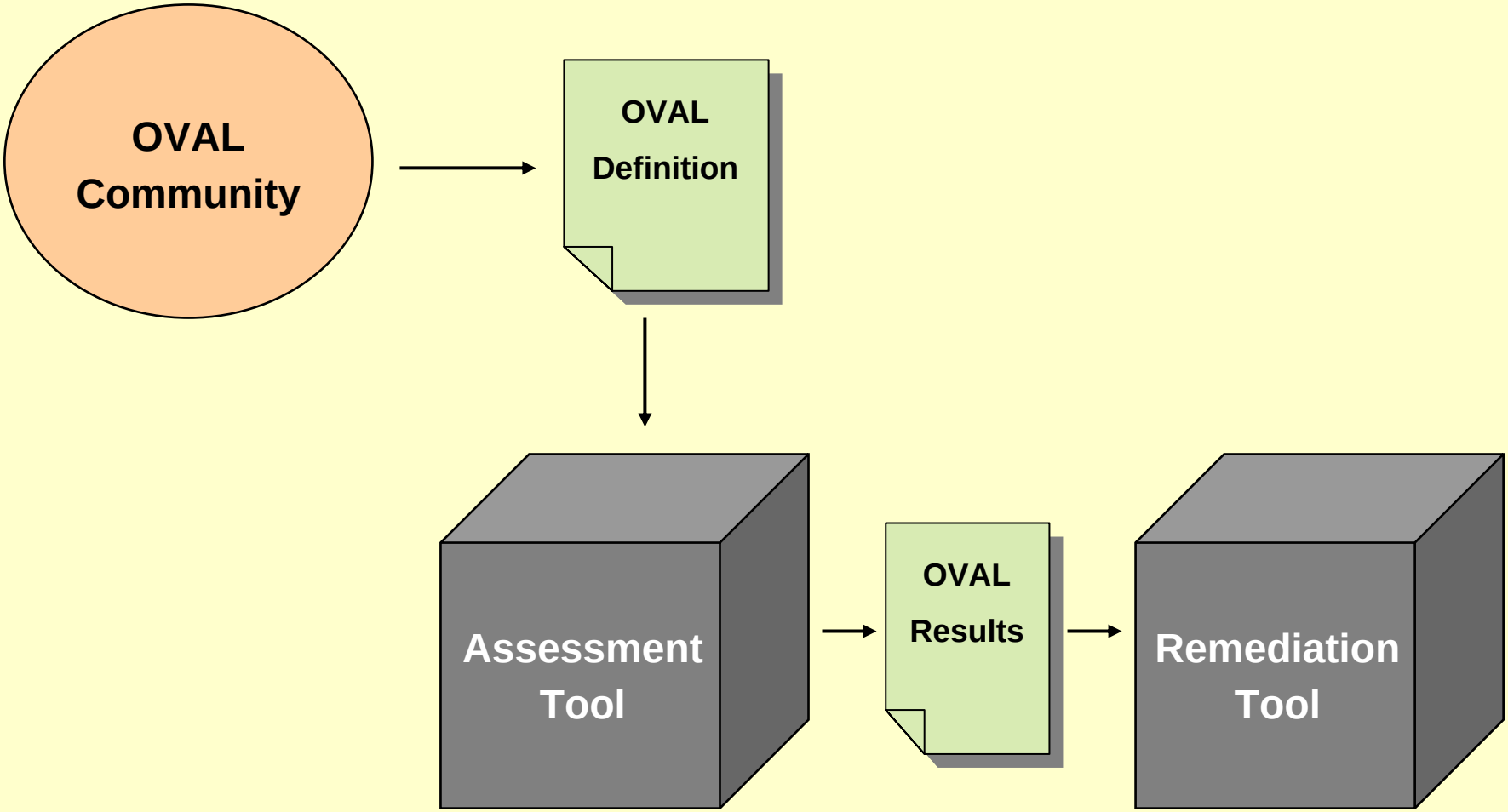
© 2006 The MITRE Corporation. All rights reserved

Configuration Management



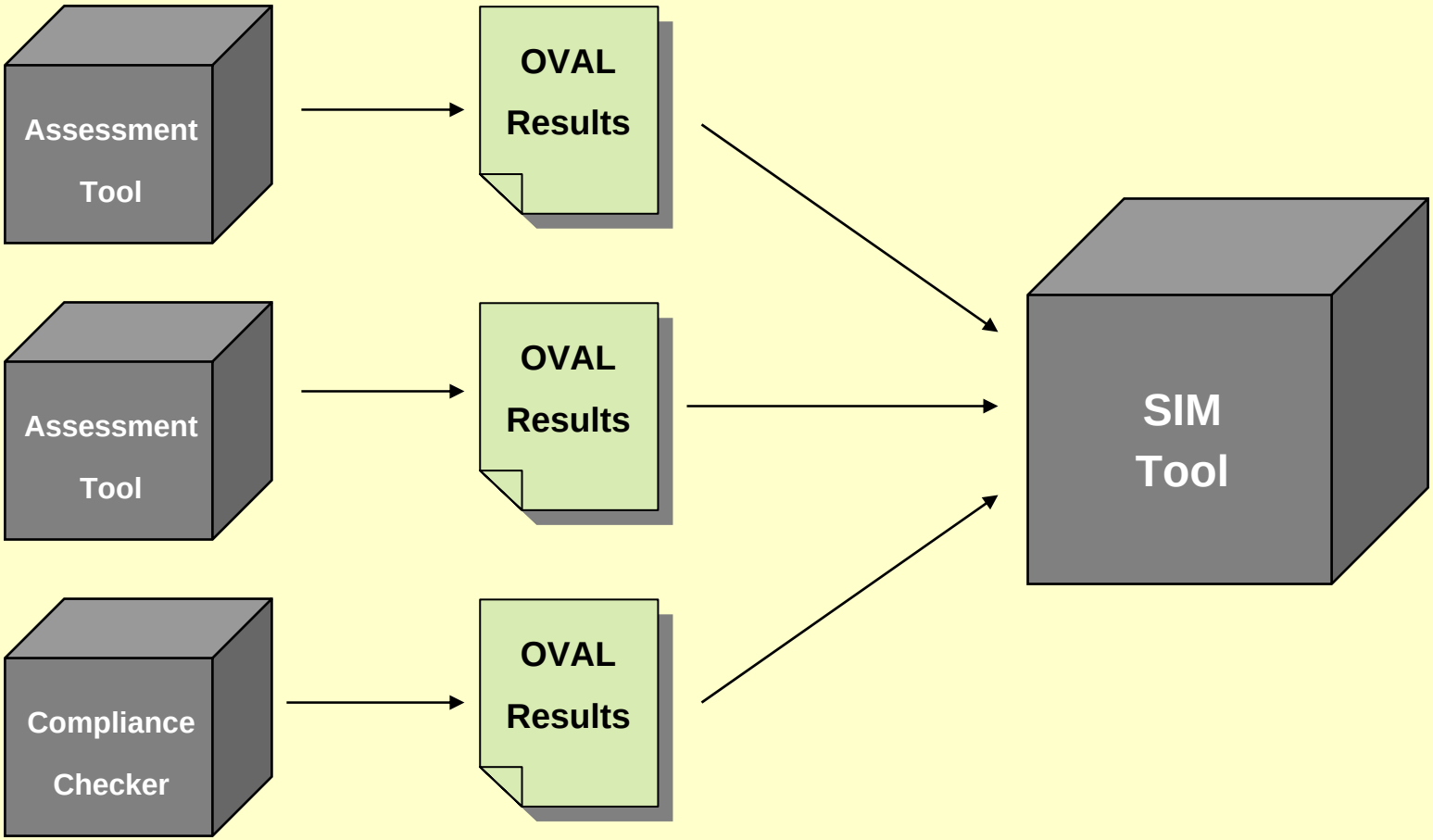
© 2006 The MITRE Corporation. All rights reserved

Vulnerability Assessment



© 2006 The MITRE Corporation. All rights reserved

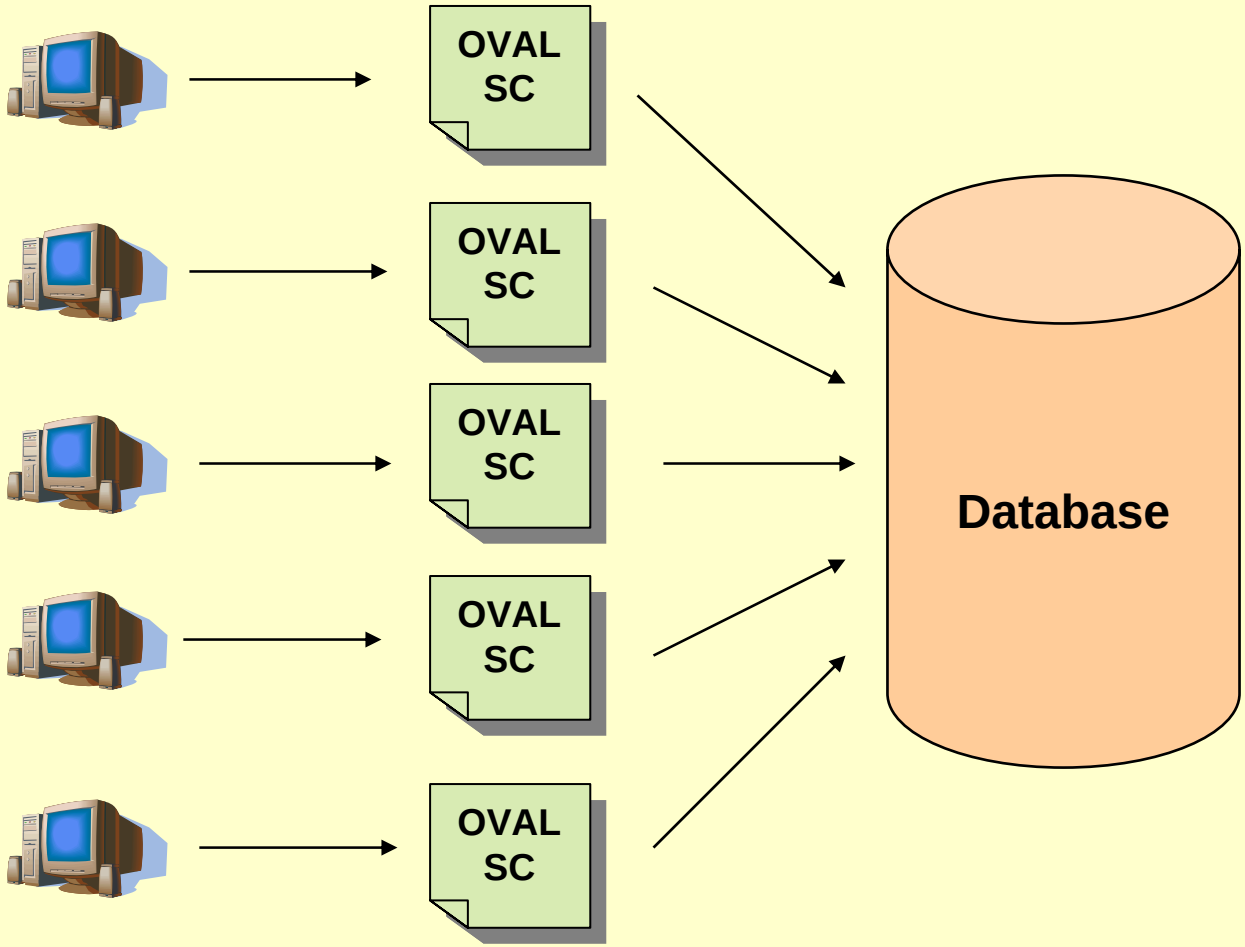
Security Information Management (SIM)



MITRE

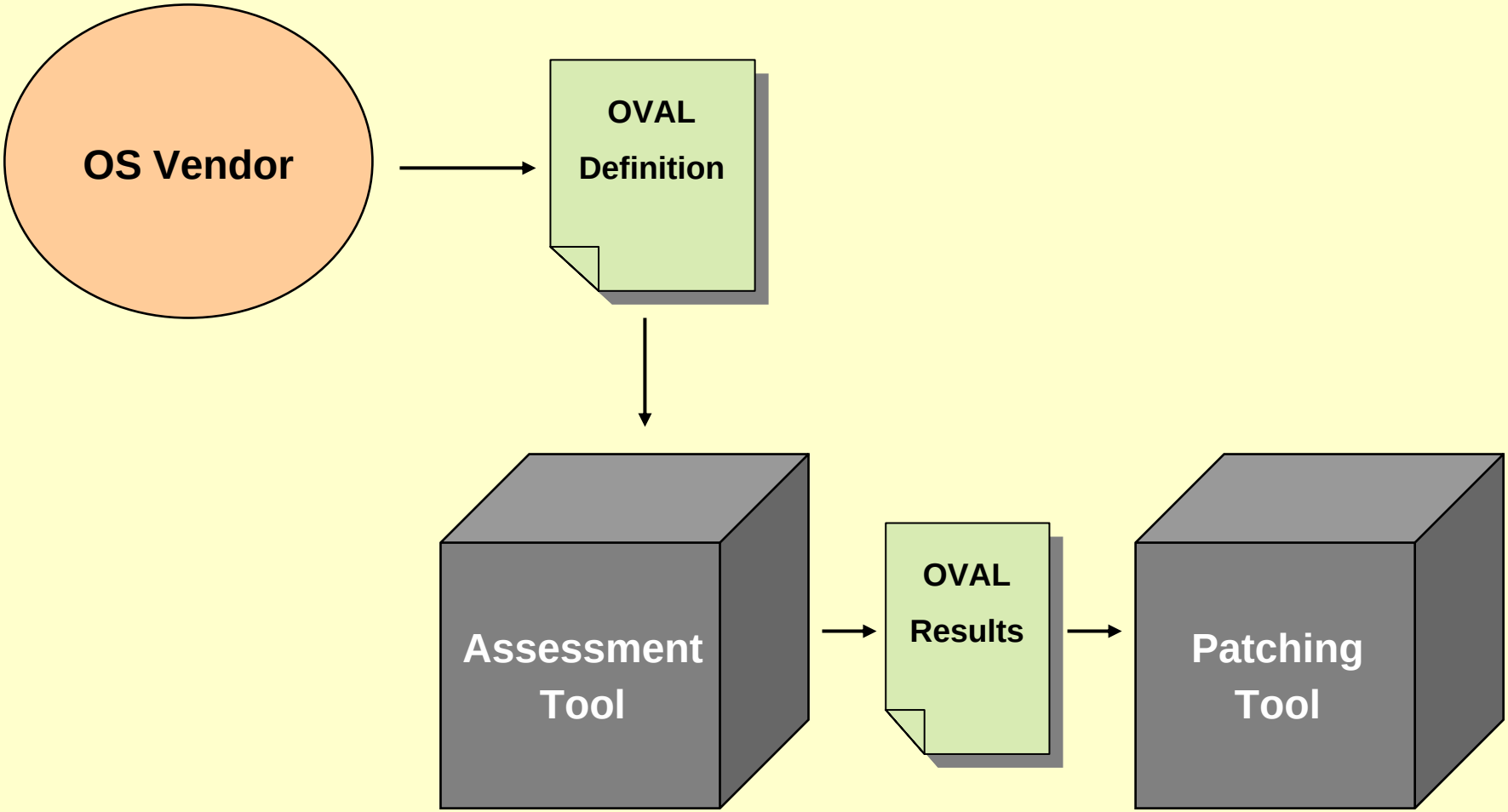
© 2006 The MITRE Corporation. All rights reserved

Centralized Audit Validation



© 2006 The MITRE Corporation. All rights reserved

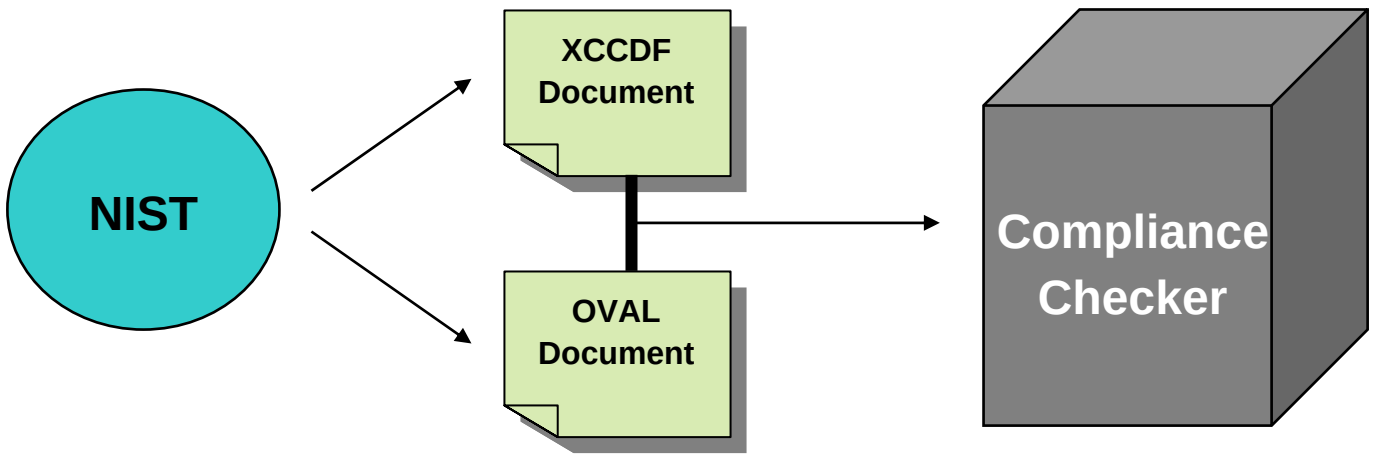
Patching Applications



© 2006 The MITRE Corporation. All rights reserved

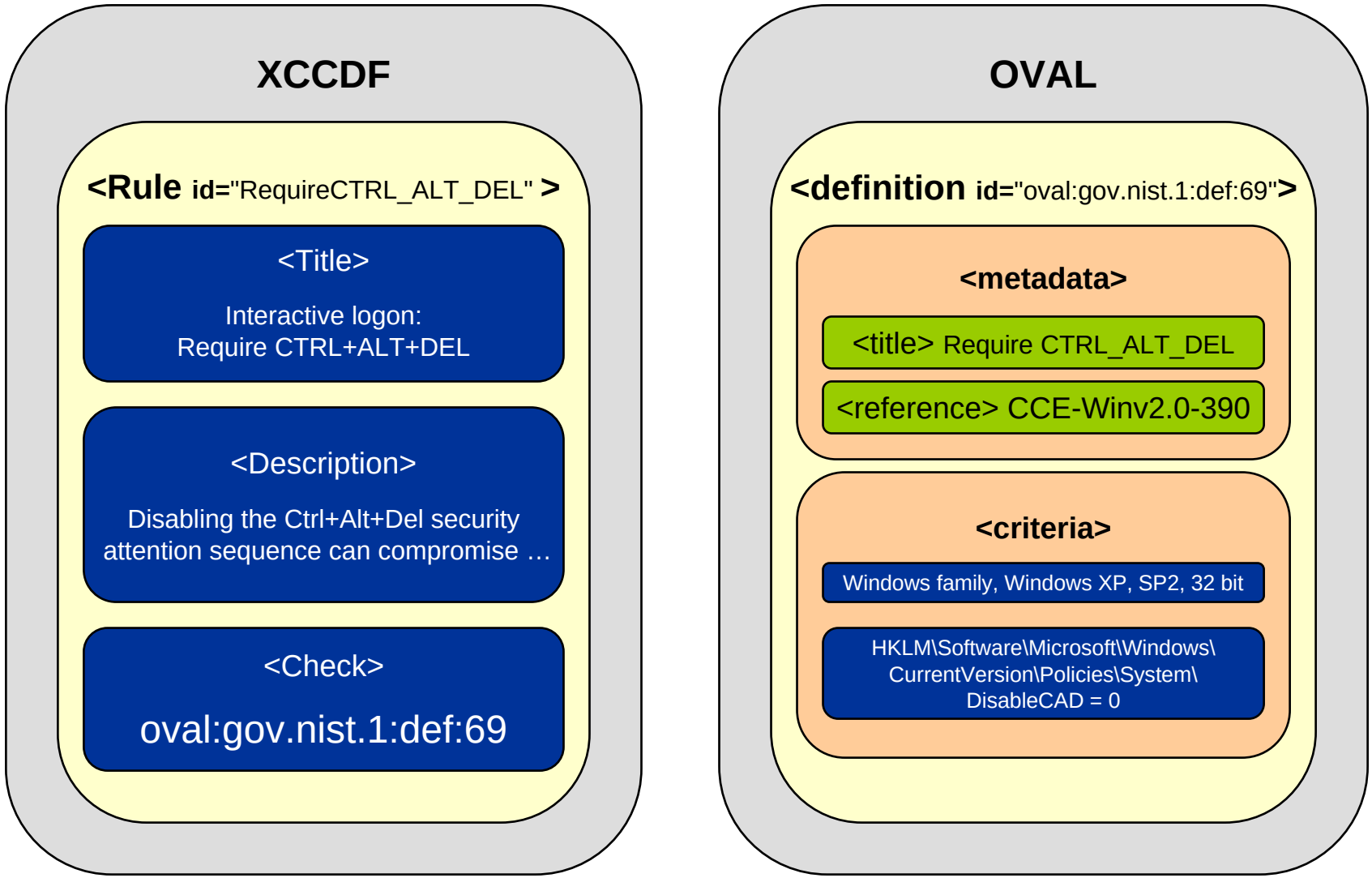
NIST and their use of OVAL

- configuration management use case
- incorporates XCCDF
- better automation than text document



© 2006 The MITRE Corporation. All rights reserved

NIST SP800-68 Appendix A – 5.28



MITRE

© 2006 The MITRE Corporation. All rights reserved

OVAL Compatibility

- **Categories**
  - **producers**
  - **consumers**

- **Dependent on schema being used**
  - **OVAL Definitions**
  - **OVAL Results**
  - **OVAL System Characteristics**

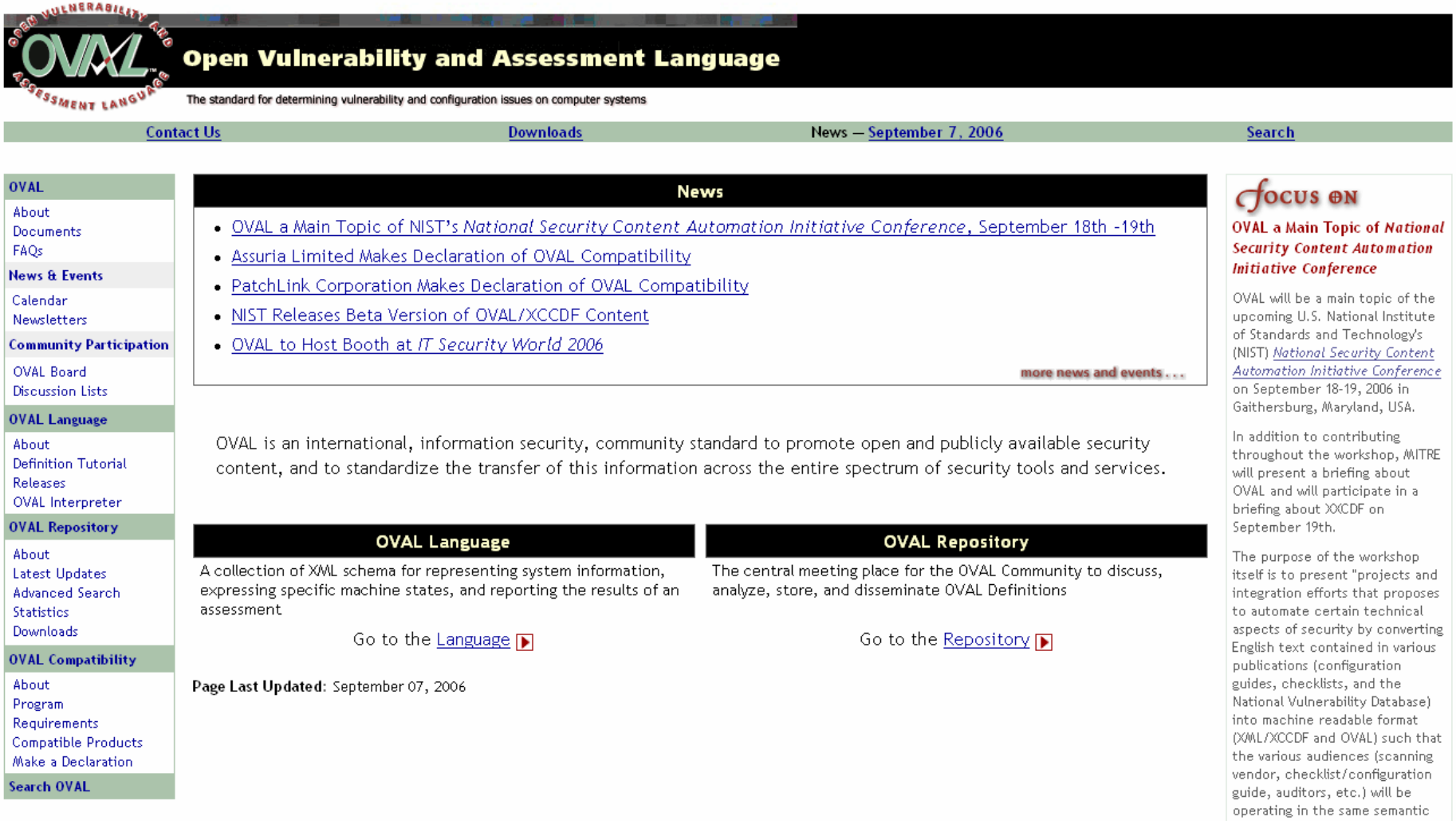
Allows customers to know which tools will work together.

© 2006 The MITRE Corporation. All rights reserved

Officially OVAL-Compatible

© 2006 The MITRE Corporation. All rights reserved

http://oval.mitre.org



Open Vulnerability and Assessment Language

The standard for determining vulnerability and configuration issues on computer systems

Contact Us | Downloads | News — September 7, 2006 | Search

OVAL
About
Documents
FAQs

News & Events
Calendar
Newsletters

Community Participation
OVAL Board
Discussion Lists

OVAL Language
About
Definition Tutorial
Releases
OVAL Interpreter

OVAL Repository
About
Latest Updates
Advanced Search
Statistics
Downloads

OVAL Compatibility
About
Program
Requirements
Compatible Products
Make a Declaration

Search OVAL

News

- OVAL a Main Topic of NIST's *National Security Content Automation Initiative Conference*, September 18th -19th
- Assuria Limited Makes Declaration of OVAL Compatibility
- PatchLink Corporation Makes Declaration of OVAL Compatibility
- NIST Releases Beta Version of OVAL/XCCDF Content
- OVAL to Host Booth at *IT Security World 2006*

more news and events . . .

OVAL is an international, information security, community standard to promote open and publicly available security content, and to standardize the transfer of this information across the entire spectrum of security tools and services.

OVAL Language

A collection of XML schema for representing system information, expressing specific machine states, and reporting the results of an assessment

Go to the Language

OVAL Repository

The central meeting place for the OVAL Community to discuss, analyze, store, and disseminate OVAL Definitions

Go to the Repository

Page Last Updated: September 07, 2006

focus on

OVAL a Main Topic of *National Security Content Automation Initiative Conference*

OVAL will be a main topic of the upcoming U.S. National Institute of Standards and Technology's (NIST) *National Security Content Automation Initiative Conference* on September 18-19, 2006 in Gaithersburg, Maryland, USA.

In addition to contributing throughout the workshop, MITRE will present a briefing about OVAL and will participate in a briefing about XCCDF on September 19th.

The purpose of the workshop itself is to present "projects and integration efforts that proposes to automate certain technical aspects of security by converting English text contained in various publications (configuration guides, checklists, and the National Vulnerability Database) into machine readable format (XML/XCCDF and OVAL) such that the various audiences (scanning vendor, checklist/configuration guide, auditors, etc.) will be operating in the same semantic

MITRE

© 2006 The MITRE Corporation. All rights reserved